EDFA
European Digital Finance Association

Initial position on PSD2 review

Our mission is to support Europe's global role in the financial technology sector.

KEY MESSAGES

- The **mandates for the regulatory bodies** ensuring the implementation of PSD2 aren't aligned with the objectives of PSD2 regarding innovation and competition.
- There are significant **discrepancies between the information available to** third party service providers **(TPPs) and what is available** in the Account Servicing Payment Service Provider **(ASPSPs) channel**. This is due partly to the lack of harmonized definitions in legal acts and interpretations of national competent authorities.
- TPPs throughout Europe are eagerly **awaiting action from regulators** and are **documenting potentially noncompliant aspects of API interfaces** and reporting this to regulators and media. ASPSPs on the other side have not established efficient best practices for responding to such reports, neither in terms of improving API functionality, nor in providing effective responses to the observations from the TPPs.
- Lack of incentives for banks to adhere to the objectives of the regulation. **Compliance as the only driver for banks** to offer viable infrastructure (APIs) for regulated third parties has proved to be insufficient.

The expectations of a frictionless open banking pan-European area prompted by PSD2 were met only half-way. To summarize the outcome from the perspective of the fintech industry in one sentence, it would be that the industry in general focused on the compliance part rather than the opportunities brought by the PSD2.

In light of the review process started by the European Commission earlier this year, members of the European Digital Finance Association have outlined the main traction points on the way to accomplish a truly thriving fintech market. These are described below in five problem domains. While some of them can be addressed by a revised regulatory framework, others are better served by the industry action, such as standards or codes of conduct.

1. PRINCIPAL PROBLEMS

European Banking Authority mandate not explicitly supporting the political objectives

The PSD2 strives to foster innovation and competition in payment services across the EU. However, its implementation relies heavily on the European Banking Authority (EBA), an authority mandated primarily to protect the "stability and effectiveness of the financial system". Although in technical terms the EBA's scope of action already includes PSD2, in accordance with Article 1 of Regulation (EU) No 1093/2010. In practice the pursuit of innovation by regulation is not well served by the current EBA objectives aimed mainly at the banking sector.

- In this regard the EBA role could be complemented with other bodies existing or created for this purpose, whose missions would be aligned more with the political objectives of the directive.

Open banking as a mere regulatory requirement

PSD2 came into force in 2018 and now, after 4 years, little innovation is seen due in part to the insufficient efforts from ASPSPs to make their APIs work at least to the level of quality standards provided by PSD2. ASPSPs have embraced the idea of opening up to different degrees. Some made large technology investments that seemed to only target the very limited scope of compliance and not the business opportunities. Others claim they do not have any incentive for embracing the digital payment scope apart from the regulatory obligation.

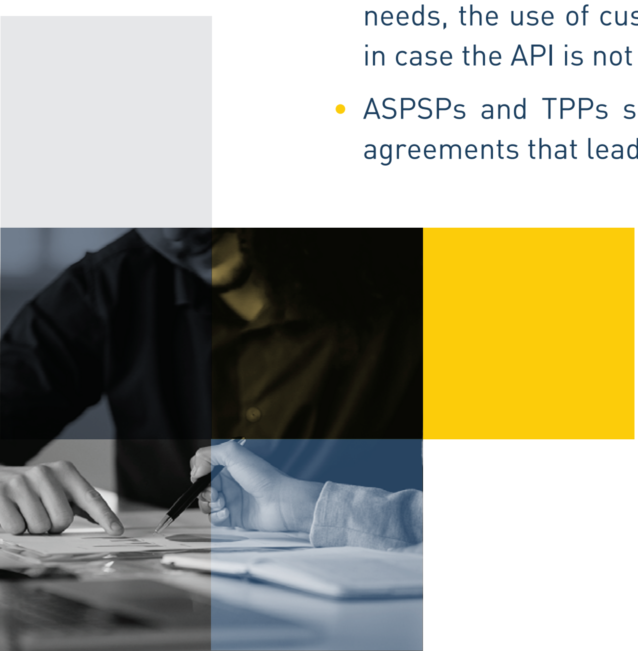
It is worth noting that one of PSD2's objectives is to improve the security of payment service users, where we should provide a more controlled technology and process integration, instead technologies presenting risks such as screen scraping or reverse engineering. However, because of the overall poor technical implementation of dedicated interfaces (APIs) and integration process of third parties , the ability to serve consumers with frictionless fintech services supported as intended by the PSD2 is hindered as is the opportunity to scale such services across the EU.

PSD2 came to address a serious issue ASPSPs own customers had been exposed to in terms of security of their data. Before PSD2 and APIs, open banking was based on credential-sharing and screen-scraping by non-regulated entities.

The security of customer data sharing should be seen as the main incentive for an ASPSP to provide a functional AIS or PIS in their API or to ensure the same level of security in the fallback mechanism. In cases where the API "only" proves responsive so that the ASPSP seems compliant and it is not providing the required quality access for the TPP to offer a viable service to the consumer, then the TPP will make use of the fallback mechanism. If the fallback interface is implemented based on screen scraping or alternative methods and TPPs end up using this interface on a regular basis as opposed to only in exceptional downtime scenarios it adds operational complexity for TPPs and is in contradiction with the objective to provide better protection for the Payment Service User.

If there is one thing that PSD2 has taught us it is that qualitative and well functional APIs are difficult to mandate. In order to create a well functioning API market, supervisory actions need to be stringent. In addition, well functioning APIs that are responding to market needs can be incentivised by ensuring that commercial interests are taken into consideration. The lack of readiness to embrace open banking and open finance by financial institutions can be approached in two ways:

- Regulate banks' use of dedicated interfaces:
    - Define a transparent EU-wide process for granting exemption by national competent authorities based on consultation with TPPs to avoid country specific interpretations.
    - Prevent ASPSPs from enabling new commercial PSU-facing payment services unless fully PSD2 compliant are provided, and ensure TPPs can make use of a fallback mechanism without access restrictions in case of non-compliance with the requirements in PSD2 of the dedicated interface.
- Ensure commercial incentives with remuneration possibilities for mandated services that go beyond the current scope of PIS and AIS:
    - The basic services of PSD2 (currently mandated PIS and AIS) should remain free of charge to further enable the entry of new players on a level playing field
    - Banks may charge a fee for new services that are mandated and go beyond the current PIS and AIS, as long as:
        - Any fee aims to foster the uptake of Open Banking, is non-discriminatory, proportionate and objectively justified, and not imposed directly on the payment service user.
        - The API is subject to the remuneration and not the service or data itselfs.
        - In order to incentivise an API market that is cost efficient and responds to market needs, the use of customer facing interfaces by TPPs shall remain free of charge in case the API is not performing or responding to market needs.
        - ASPSPs and TPPs should adopt a scheme to avoid the need to enter bilateral agreements that leads to scaling issues and unnecessary burden.



2. SCOPE AND DEFINITION PROBLEMS

Insufficient exemption conditions for electronic communications providers

Article 3 (l) of PSD2 provides exclusions for the electronic communications providers (ECP). They include digital content, voice-based services, tickets and charitable activities such as donations. This scope is rather casuistic and narrow as it does not take into account digital services portfolio growth, which is a hindrance to innovation. We propose the following:

- A non-casuistic regulatory approach might be considered where the focus is laid on the specific characteristics of the purchase (payment transaction initiated by electronic device at the operator, the payment transaction is executed by the operator, consideration charged by the operator to customer's bill or deducted from customer's balance issued by operator etc.), instead of defining the scope of related products or services covered by ECP.
- It might be also considered to define the scope to include new similar digital content/ services with a physical element, too (e.g. delivery subscriptions). Further, in regard to innovative services and products with digital elements the regulatory framework of digital content, digital services, goods with digital elements as laid down by the DCSD -Directive (EU) 2019/770- might be taken into account.

Thresholds for single payments and cumulative payments under the ECP exemption

Even before the Covid-19 pandemic consumer behavior and needs were changing towards a strong preference for use of e-commerce and electronic payments. For that reason:

- The system of thresholds under ECP requires a review based on the analysis of current market conditions and consumer habits.

Unequal definition of AISPs and PISPs

Nowadays, in some countries, AISPs and PISPs are considered as technology enablers and not as financial institutions. This inevitably generates a disadvantage in terms of costs and customer journey for these market players defined as financial institutions and thus treated as obliged under AML requirements.

The European Banking Authority took a strong stance on this topic, issuing the revised guidelines on ML/FT risk factors (EBA/GL/2021/02, March 2021). In the sectoral Guideline for PISPs and AISPs (GL 18), EBA clearly states that these new players are obligated entities under Directive (EU) 2015/849 but also that the inherent ML/TF risk associated with them is limited. This position is confirmed in the Q&A area (Feedback on responses to Question 18). To account for this, we propose that:

- Obligations for AISPs and PISPs should be limited and proportional to the real services they offer.
- For PISPs, all information necessary to do proper transaction monitoring is still not always provided by the ASPSPs (see discussion in point 5), which makes it impossible to comply with the AML regulation without heavily impacting the customer journey.
- For entities providing the service of AIS on a one-off basis (e.g. in case of aggregation of account information for creditworthiness assessment purposes, in order to obtain a quote for a loan), the application of AML/CFT obligation towards the end client should be expressly excluded, considering that (i) no on-going business relationship is established with the latter; and (ii) there is no transfer of funds through the AISP.
- AISPs have access to multiple sources and therefore have a privileged position in monitoring fraudulent schemes compared to individual ASPSPs (e.g. funds transfers from different payment accounts to the same payee). However, detecting such a pattern (grand smurfing), would mean the AISPs would need to scan through the transaction history of all connected accounts for a PSU, which is a disproportionate effort compared to the gain for the financial sector. AISPs don't have the resources to perform such checks and since this is the only potential risk, we recommend introducing an exemption to AML for AIS services. For this reason, transaction monitoring should be the only obligation for these entities.
- Many PISPs have a merchant-facing model where the PISP offers payment initiation to the merchant. In this case, the PISP enters a business relationship with the merchant who is the payee/beneficiary of the payment. For AML/CFT obligations the only customer of the PISP should be the merchant and not the merchant's customer, the payer. Therefore customer due diligence obligations should apply only to the PISP of the merchant.

Implementation of commercial agent exclusion for B2C e-commerce platforms

According to the implementation of commercial agent exclusion for B2C e-commerce platforms, EBA stated in their statement (Q&A 2020 5355) that a business-to-consumer (B2C) e-commerce platform could be excluded from the scope of PSD2 if, as a commercial agent, it is authorized by the payee to negotiate or conclude the sale of goods or services and if it does not also act on behalf of the payer. However, as the EBA itself highlights, PSD2 does not provide criteria in order to determine whether a platform can be deemed to be also acting on behalf of the payer. This leads to numerous interpretations across the EU and disparities in the market practice, which hinders the harmonization and a level playing field in the payment service space.

- Conditions defining when a platform is deemed to act on behalf of the payer should be part of the legislation, in a revised payment services directive or in other relevant legislation.

Triangular passport

The "triangular" passport is a situation in which a payment services provider (PSP) licensed in country A entrusts a PSP agent located in country B in order to provide payment services in country C. As noted by French Prudential Supervision and Resolution Authority (ACPR) in the Q&A 2021_5726 to the EBA, practices around the triangular passport are not harmonized across EU countries since certain member states notify triangular passport based on the intermediary of a PSP agent, while other reject or do not simply notify such passports, creating an unlevel playing field in the EU.

- We suggest to expressly provide that a PSP licensed in country A can avail itself of a PSP agent located in country B in order to provide payment services in country C, by notifying its own Authority that will, in turn, notify the two host Authorities. In this case, it would also be helpful to clarify which would be the law applying to the PSP agent's activity, for example as to AML/CTF. Second best option would be to introduce an ad hoc passporting procedure for PSP agents, in the same fashion as for insurance distributors

Scope of the information that can be accessed by TTP

PSD2 is silent on access to other types of information than the information from payment accounts and associated transactions (Article 4(12), Article 4(5), EBA opinion on RTS). However, the general principle under PSD2 is that the ASPSP should enable the same type of access to accounts that it provides within its own digital channels. Most ASPSPs currently allow their retail or business customers to check multiple types of accounts in their own digital interfaces. The scope of PSD2 becomes thus defined by the ASPSPs definition of types of accounts and the regional interpretations.

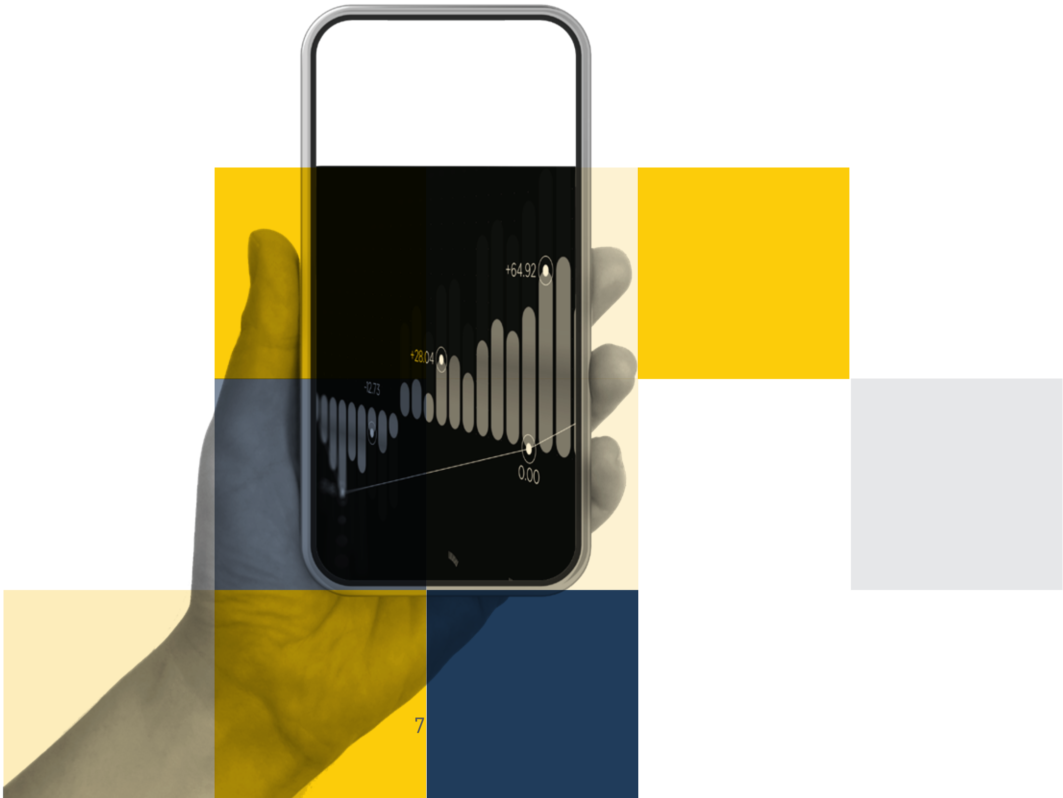
As the interpretation of what the ASPSP considers to be an account regulated under PSD2 vary from market to market and ASPSP to ASPSP, regulation should provide consistency across Europe as to what types of information should be made visible through the account information API or supported by the payment initiation API, provided they are already visible in the online banking application. ASPSPs should be obliged to enable access to and operations from those types of accounts that it aggregates in its own digital channels (mobile/ online banking apps), i.e. deposit accounts, credit accounts, overdraft accounts, POS accounts, direct debit pooling accounts (ie: used by utility companies to collect their debts).

- ASPSP aggregation of information should be made visible through the ASPSP API

PSD2 to better address current developments and market needs

PSD2, and the definition of PIS specifically, were defined and tailored for traditional e-commerce. Since then it has also been adjusted for m-commerce with some clarifications by the EBA. However, the digital economy where the consumer is not present using a desktop or mobile phone is ever growing and in need for further innovation. There is currently no real possibilities to provide PIS in any other context than traditional e- and m-commerce, e.g. IoT, Voice recognition services, Metaverse, smart contract based payments, proprietary or closed loop systems that aren't app or browser based, etc.

- Make sure that the legislation pertaining to payment services addresses trends and consumer needs in the payments market to foster adoption of PIS in the wider digital economy.
- Make SCA exemption to trusted beneficiaries (art. 13 in RTS) mandatory to foster adoption of PIS in the wider digital economy, together with a consent model for consumer protection and transparency.
- Foster the adoption of flexible payment services (e.g. variable recurring payments).
- Ensure payment certainty for PIS both immediate and future dated payments.



3. GOVERNANCE AND IMPLEMENTATION PROBLEMS

Inefficient API obstacles reporting

PSD2 requires ASPSPs to provide dedicated interfaces for regulated third parties (TPPs) with functionality and quality equal to what is provided in the ASPSP's own channels. As this is a regulatory requirement, the normal partner relation between the ASPSP and TPPs is somewhat challenging because they are often direct competitors.

Fintechs (TTPs) throughout Europe are eagerly awaiting action from regulators and are documenting potentially noncompliant aspects of these interfaces in numerous ways, and reporting this to regulators and media. ASPSPs on the other side have not established efficient best practices for responding to such reports, neither in terms of building functionality that is found to be lacking, nor providing effective responses to observations from the TPPs.

Regulators would benefit from better and more standardized documentation of perceived or actual noncompliance from both ASPSPs and TTPs alike, enabling them to focus regulatory priorities and operate more efficiently. For that purpose:

- Establishing standardized measures to notify obstacles and manage disputes efficiently would be beneficial to the industry as a whole. Market players should commit to a code of conduct (such as the 33report.eu initiative), where API obstacles are immediately reported to the ASPSP, relevant supervisory authority(ies), and the industry itself in an open manner.
- A statutory alternative to an SLA (Service Level Agreements) should be established with the ASPSPs and tangible engagements for response time and obstacle/disputes resolving should be defined.

Lack of transparency of ASPSP PSD2 API's availability and performance

Most ASPSPs do not use the dedicated interfaces for supporting their own payment services. The availability of the dedicated interfaces will typically not be monitored by the ASPSP offering them as well as the APIs they use for their own payment services. To improve the situation the following steps should be taken:

- Introduction of additional incentives for ASPSPs to ensure appropriate service levels of the regulated interfaces are beneficial.
- Benchmarking of the availability metrics in an open manner, accessible by all TPPs
- Standardizing the communication for notifying insufficient availability of account services including the indication of the impact level to ensure appropriate prioritization by the ASPSP.
- ASPSPs should explicitly notify subscribed TPPs for every change, using a standardized, structured and clear process before the production rollout (automated email should be the default).

- Some markets and aggregators have established dedicated monitoring services provided to the community at large. In Romania for example the National Bank is using a monitoring tool, built as a collaborative initiative between market players. The tool is a managed service, it has monitoring features over the PSD2 ASPSPs's production APIs and it was launched at the beginning of 2022; it provides continuous monitoring and reporting. This kind of initiative can be replicated at a larger scale, at each country level and it would be a useful mechanism to improve transparency over the PSD2 APIs.

In most countries, the burden of proof of ASPSP API unreliability is on the TPP. This is rarely possible since a single TPP is only one part of the traffic for an ASPSP and therefore not always representative. Moreover, the amount of time and investment needed to provide the thorough reporting NCAs ask of TPPs to consider a case is way too expensive for new entrants, with the consequence that new entrants with innovative solutions prefer to move away from PSD2 and stop their business. ASPSPs are, on the other hand, supposed to report on the availability of their APIs to their NCA.

- Reporting should be available to all PSD2 regulated parties and that the burden of proof be put on ASPSPs instead of TPPs that don't have the resources to do it properly.

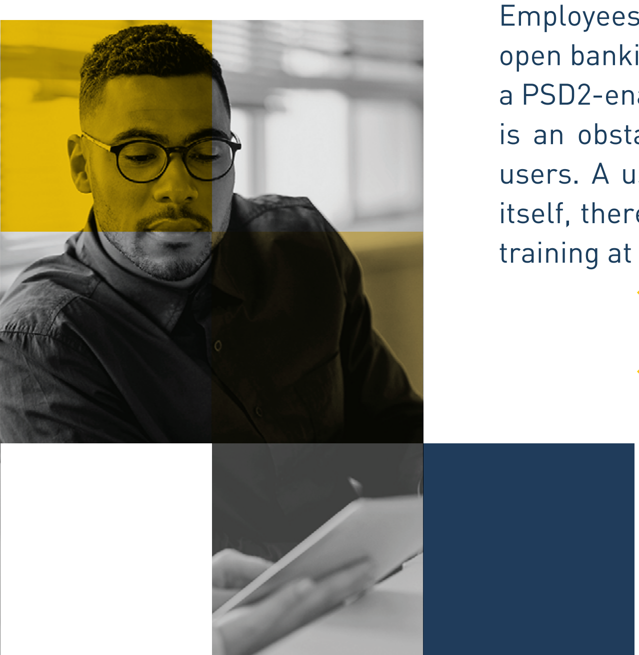
Inefficient API notifications to TPPs

When changes are planned or occur due to mitigating operational actions, ASPSPs do not always provide information about it in a standardized manner. Some ASPSPs provide changeboards at the websites of the ASPSPs, making the efforts by the TPP inefficient with regards to monitoring all websites.

- Regulators should impose a common practice to push such notifications (email as default) as well as an agreed timeframe to do so in order for TPPs to be able to adapt.

Lack of proper information about open banking services

The financial industry and the relevant supervisory authorities communicating with consumers or relevant other stakeholders on the consumers behalf do not always have the competence needed to explain open banking services and underlying regulatory trust in a trustworthy manner. As a consequence, the end-consumer may perceive the third-party offerings are fraud and the trust that should normally be provided through the regulatory framework is missing.



Employees outside technical departments are not always aware about open banking/PSD2 services. When a customer is having a problem with a PSD2-enabled payment, the call center will not be able to assist, which is an obstacle in building PSD2 trust and supporting adoption among users. A user will not trust a service that is not known by the ASPSP itself, therefore it should be mandatory for ASPSPs to perform relevant training at call centers and front-end offices.

- ASPSPs should provide proper open banking training for their employees.
- The EBA TPP registry could be extended as a source of known regulated entities for ASPSP support agents provided that the names of the various products operating behind the same company name mentioned in the registry are also present.

Slow and unpredictable Q&A response time for clarifications

Questions and interpretations sent to EBA have been processed at a phase not aligned with the demand from the market. Innovators or ongoing processes have been stalled for months and sometimes years to clarify regulatory conditions in the PSD2 framework. The reply time was often more than six months, in several instances it took years to prepare a reply[1].

- EBA should be mandated to issue clarification in a timelier manner.
- Where more extensive and time-consuming analysis needs to be performed before being able to produce an answer, a communication forecast or principal deliverable might add value.

[1] Examples of EBA reply time:
https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6236 • Date of submission:12/10/2021, Published as Final Q&A: 13/04/2022,
https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4081 • Date of submission: 04/07/2018 Published as Final Q&A: 25/01/2019,
https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2021_6235 • Date of submission: 12/10/2021. Published as Final Q&A: 13/04/2022,
https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5165 • Date of submission: 09/03/2020. Published as Final Q&A: 18/03/2022,
https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4096 • Date of submission: 10/07/2018. Published as Final Q&A: 21/01/2022.

4. API GENERIC AND INFRASTRUCTURE PROBLEMS

Standardization of transactions information

As opposed to other digital channels, ASPSPs only provide limited or partial transactional data. The majority of these distinctions can be found in the transaction description as the complete description is available on the internet or via mobile banking. Some ASPSPs create additional obstacles by implementing an additional request to get the full transaction description. Missing information during payment transactions, which is owing to standardization of bank transaction information, substantially lowers the quality of the services provided by TTPs. Therefore:

- A revised legislation should define the minimum of information that ASPSPs are supposed to provide in a structured way during payment transactions and in the account history.
- Alternatively, legislation should at least include specific requirements for non-discriminatory measures and oblige the ASPSPs that data shared are the same as the one available in IB or MB.

Lack of automated onboarding for end consumer

In some counties, eg. Romania and Croatia, offline interventions with the ASPSP are required before online onboarding of the customer. For corporate users, some ASPSPs explicitly require all their corporate users to ask for specific access enablement in order to be able to connect the accounts on which they are mandated in the IB, or they do not support an authentication method compatible with the regular authentication used by the corporate user. To improve the situation:

- TPPs should collect and analyze all instances of consumers or companies, who are not automatically authorized to perform an SCA. This will allow the TPP to establish if the ASPSP follows a general rule for how the API access was implemented by those ASPSPs. Assess the impact of these rules on end users, against the considerations of EBA on what may represent obstacles to users access to the API. Based on the evaluation, ask EBA to provide more clarity on these obstacles and enforce the RTS.
- ASPSPs should stop preventing PSUs to access AIS services on a basis that new mandates need to be signed, or in the case this is justifiable, they must provide a clear procedure to follow on their website or customer facing documentation so TPPs can refer the PSU to it.
- The ASPSP should not ask for TPP IPs whitelisting as part of onboarding. This is also a major obstacle since it can take quite a lot of time for ASPSPs to do such whitelisting and in case the TPP's technical network address changes, there is a high risk of service discontinuity.

Unequal TPP registration with the ASPSPs development and live XS2A portals

On the market, the ASPSPs have taken different approaches to the TPPs registration processes: some are totally automated, while others require email as a communication channel. All of the processes end with application approval, but the response time needed for the ASPSP confirmation differs substantially. Moreover, the situation is aggravated by the lack of standardization as to the documentation and digital certificates required by the ASPSP in the registration process. For example, some require VAT numbers, scanned copies of publicly available documents and there is no certain rule which digital certificate should be used for the TPP identification. We observe that most of the ASPSPs require just the QSeal certificates, while others require both QSeal and QWac. This unnecessary burden can be addressed by:

- Harmonization of the ASPSP registration process requirements by including an explicit listing in the RTS Providing documentation and digital certificates required by the ASPSP, timeframes for the ASPSPs to confirm the registration and mandating efficient and seamless procedures for lifecycle management of certificates

AIS calls limit constraints market developmentt

As of now there is a maximum 4 calls per day limit when the TPP is calling PSD2 AISP APIs and the end user is not online. This limit should be reconsidered.

- Possible solutions include removing the limit altogether or creating a common standard or a more unified market best practices (such as API rate limiting for instance) where limits can vary depending on the TPP and moments in time.
- Alternatively, setting the limit at partner level would also help: if a regulatory shielding TPP has 3 partners accessing the same accounts, the maximum limit should be applied at each partner level. "Otherwise, the partners will remain eventually with no offline calls available as the 4 calls per day limit is at TPP level.)"

Uncoordinated SCA renewal

Today, most TPPs see a drop of customers at every SCA renewal. One reason provided by PSUs for abandoning a TPP service is that renewing their SCA is just too cumbersome. To avoid that:

- The best solution would be to remove the SCA renewal requirement as a whole, or to at least consider it for business accounts. The rationale behind this removal is backed by the fact that business ASPSP account integrations (for example accounting and ERP solutions) have, in some countries, already worked for years, without a SCA renewal requirement. It has never led to issues, proving that the risk is not there. If the underlying rationale for the requirement is to protect the payment service user against forgetting that an AIS integration is still used, then this is more applicable to the consumer space and the SCA renewal requirement should therefore be limited to consumer accounts only.
- Alternatively, it should be enough for the TPP to provide simple proof to the ASPSP that the consent of their payment service user was renewed to obtain a new valid connection token to the ASPSP API. This would mean delegating the SCA renewal to the TPP.

Regulated TPPs should be trusted and, based on renewed consents from their customers, allowed to continue using the API without additional SCA at the ASPSP.

- As a compensating measure for removing the SCA renewal requirement, it could be considered to oblige the ASPSP to inform the payment service user every 180 or 365 days about active connections, with the option to disable the connection from the ASPSP's channels.
- An alternative approach, would be to enable the payment service user to disable the SCA renewal requirement in the AIS consent flow, i.e. explicitly requesting the ASPSP to not apply this, putting the PSU in complete control over when to apply SCA. We believe it can be reasonably expected from an PSU to take on this responsibility, which would result in a significant improvement of the UX for the payment service user in other words: it would remove one of the most significant frictions that is currently impeding the success of PSD2.

5. DISCREPANCIES BETWEEN INFORMATIONAVAILABLE TO TPPS AND WHAT IS AVAILABLE IN THE ASPSP CHANNEL

No access to credit card balances and transactions

In certain EU member states supervisory authorities interpret that credit card balances and transactions should not be provided to TPPs by ASPSPs through their dedicated interfaces. This is justified through a myriad of inter-relations between different EU directives and through the lack of clear definitions of basic concepts, such as what is a payments account.

- In order to bring consistency for the PSU across Europe, any future legislative act relating to open banking and open finance should have non-interpretable and clear definitions of the basic elements it regulates as well as its attributes.

Lack of information about the account owner

For the account information service, the account owner name is not always provided. Similarly, the payer name is not always provided in the payment initiation services. Even though it has been clarified by the EBA that this information must be available to TPPs if it is shown in the ASPSP interface. This hinders the potential of use cases for which there is significant demand on the market, such as identity confirmation as part of risk scoring for example.

- Regulators should make sure this information is provided by the ASPSPs in order to support adoption and PSD2 services development. Such disclosure should comply with GDPR rules and be based on explicit owner's consent. With account owner information available, better AML checks could be done on the TPPs side.

Insufficient transaction history length

Transaction history available though PSD2 should be the same as the one available in IB or MB as long as there is an active consent For example, some ASPSPs set the available history interval to the remaining active consent period.

- Transaction history period should at least be the same as the one available in IB or MB, and provide least 12 months of history.

Differences in ASPSP development/sandbox interface and live/ production

There are major differences between what the TPPs can test in the development or sandbox environment and what is indeed working in live environments. For example some ASPSPs allowed the entire corporate functionality in a sandbox but not in a live interface. In real production use, this is an important obstacle because TPPs cannot properly test some specific fixes related to behaviors that can be replicated only in production. The strategy of "deploy and test" directly on productions brings additional risks and negative impact on customers.

- ASPSP should assure that sandbox environment has the same behavior as the production one in terms of: onboarding, SCA, payload structures, consent management and lifecycle.

Unequal mobile onboarding process between ASPSP and TPP

In most cases the mobile journey for TPP service users is not the same as the one the customer goes through their native mobile banking app. "For example, (while MB accepts biometric authentication the PSD2-enabled service requires a web browser with additional credentials and a bad user experience." A smooth and flawless user experience is essential for PSD2 adoption, otherwise existing traditional channels will be preferred.

- The ASPSPs should offer the same authentication features and user experience as the one they have on traditional channels, without additional or unnecessary steps.
- In the redirect scenario, the user experience should be the same as the one on the ASPSP's traditional channels. Some users abandon the flow because the ASPSP interface is looking different, sometimes unfinished in terms of design. The users can have the feeling that this is not the ASPSP's genuine interface.

Certain payments by TPPs are not supported by ASPSPs

ASPSPs that provide either bulk, recurring, and/or future dates payments do not at all offer it to TPPs. Some ASPSPs still claim it is optional because standards like Berlin group or others mark it as optional.

The EBA has clearly stated in their last Q&A that a TPP has the right to initiate the same transactions that the ASPSP offers to its own PSUs, such as instant payments, batch payments, international payments, recurring transactions, payments set by national schemes and future-dated payments. However, in practice, some ASPSPs still do not.

- Regulators should ensure that all NCAs have the same interpretation and enforce the EBA's final answer.

Exemption from SCA for certain automated payments

There are use cases in which at this moment PSD2 services can not be used because it would be required to have in-place payment authorization exceptions functionality. Ride sharing might be an example, or any other scenario in which the user can not authorize the payment at the very moment when it needs to be performed.

- Exemptions from SCA should be implemented on low value payments and trusted beneficiaries.

EDFA
European Digital
Finance Association

The report was drafted by EDFA's working group on payment services and is meant to trigger a wider market discussion about the ongoing PSD2 review process. We invite all stakeholders to contact us for further exchange of views and positions.

European Digital Finance Association is an independent industry body that represents the European digital finance community. It unites fifteen European national fintech associations, and thus their several thousand members covering a wide range of companies from startups and financial institutions to investors and professional services companies.

Our mission is to support Europe's global role in the financial technology sector.

CONTACT
Niklas Sandqvist, Chair
Working group on payment services
niklas@europeandigitalfinance.eu